



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450.
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,111	03/25/2004	Jonathan Wilkins	MS#307312.01 (5104)	6640
38779	7590	08/10/2007	EXAMINER	
SENNIGER POWERS (MSFT) ONE METROPOLITAN SQUARE, 16TH FLOOR ST. LOUIS, MO 63102			YOUNG, NICOLE M	
ART UNIT		PAPER NUMBER		
2139				
NOTIFICATION DATE		DELIVERY MODE		
08/10/2007		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

mN

Office Action Summary	Application No.	Applicant(s)
	10/809,111	WILKINS ET AL.
	Examiner	Art Unit
	Nicole M. Young	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 March 2004.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-40 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-40 is/are rejected.
- 7) Claim(s) 14,20 and 40 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 25 March 2004 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This communication is in response to the application filed on March 25, 2004. Claims 1-40 are currently pending. The Applicant has used the phrase "means for" within the claim language. The Examiner considers 112 6th paragraph to be invoked.

Claim Objections

Claims 14, 20, and 40 are objected to because of the following informalities:

The claims state "an result" which is not grammatically correct. Change "an result" to "a result" in all claims.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1, 16, 26, 33 are non-statutory because they do not produce a tangible result. These claims end with comparing data, determining, or analyzing data. This does not provide a tangible result. A tangible result would include what is done with the data after a positive and negative comparison or determination.

Claims 8-10, 21, 22, 25, 28, 29, and 36-38 are dependent claims that do not further provide a tangible result.

Claims 8-10, 21, 22, 25, 29, and 36-38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 8, 9, 21, 22, 25, 29, 36-38 are non-statutory because they include a non-tangible result in the case that the identified requests do not indicate the characterized attack. **Claim 10** is a dependent claim and does not further provide a tangible result.

Claims 25 and 32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims use the language "means for", therefore they must have specific tangible hardware components in the specification.

Claims 15 and 33-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Generally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. See MPEP § 2106 IV.B.I(a). However, in the present application, the specification defines "computer-readable media" to include, for example, paper or various communication media as on page 33 of the specification. A computer program listing on a sheet of paper is not considered to provide functionality, and is therefore considered to be merely a computer program per

se, which is non-statutory subject matter. Further, "communication media" includes non-tangible media such as signals as on page 34 of the specification. When a claim encompasses both statutory and non-statutory subject matter, the claim as a whole is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5, 8-10, 13-17, 20-22, 25-27, 29, 30, 32-34, 36-38, 40 are rejected under 35 U.S.C. 102(e) as being anticipated by **Bruton, III et al. (US 2003/0145225)** herein referred to as Bruton.

Claims 1, 15, 16, 26, 30, 32, 33 disclose a method of detecting an attack on an authentication service, said method comprising:

storing data relating to a plurality of requests (Figure 3, IDS Mgmt System 300 and associated text, also see Figure 4, 410) as communicated to an authentication service from a plurality of user agents via a data communication network (Figure 3 shows multiple agents such as 230, 240 and 310 communicating with 300 over networks),

searching the stored data based on a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user

agents (Paragraph [0057] wherein the packets are the stored data and the signature file is interpreted to be the query variable), and

comparing the stored data associated with each of the identified requests with a predefined pattern characterizing an attack to determine when the identified request indicates the characterized attack on the authentication service (Paragraph [0057]), the data is compared against the specific attack signatures which are interpreted to be predefined patterns characterizing an attack).

Claims 2, 17, 27, 34 discloses the method of claim 1, wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which one of the plurality of the requests is communicated (Paragraph [0060] teaches address spoofing); a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests (Paragraph [0074] where the IDS functions on the application layer) ; a status of the one of the plurality of the requests (Paragraph [0029], wherein the conditions are interpreted to be the status of the event); a time stamp indicating a date and time of the one of the plurality of the requests (Paragraph [0035] teaches a date and time timestamp); a type of interface from which the one of the plurality of the requests is communicated; and the user agent from which the one of the plurality of the requests is communicated (Paragraph [0074] where the IP headers are interpreted to be the user agents).

Claim 3 discloses the method of claim 2, wherein said status of the one of the plurality of the requests comprises one of more of the following: the one of the plurality of the

requests is successful; the one of the plurality of the requests is unsuccessful; and the user account associated with the one of the plurality of the requests has been locked (Paragraph [0068] teaches denying or discarding traffic that is determined to be related to an intrusion attack. This is interpreted to be a unsuccessful request).

Claim 5 discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using a single password to unsuccessfully attempt at least a predetermined quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the multiple user accounts within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the single network address within the predefined time interval (Paragraph [0061] where the number of events from a single source are compared to a threshold).

Claims 8, 21, 29, 36 discloses the method of claim 1, further comprising generating a report if it is determined that one or more of the identified requests indicate the characterized attack, said report providing information regarding the attack for use in defending against the attack (Paragraph [0068] teaches reporting the intrusion events so that defensive action can be taken).

Claims 9, 22, 25, 37 discloses the method of claim 1, further comprising remedying the attack if it is determined that one or more of the identified requests indicate the

characterized attack (Paragraphs [0068] and [0069] teach reporting the actions and ways to remedy the attack).

Claim 10, 38 discloses the method of claim 9, wherein said remedying the attack comprises performing one or more of the following: locking a user account associated with one of the plurality of the requests; blocking a network address from which the one of the plurality of the requests is communicated; implementing a human interaction proof on the authentication service; prompting a user to change a password associated with the user account; and limiting a quantity of allowed unsuccessful requests to a predetermined quantity within a predefined time interval for the network address from which the one of the plurality of the requests is communicated (Paragraph [0068] teaches methods of real time defensive actions in response to the attack).

Claim 13 discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with a predefined pattern comprises: comparing historical data relating to the authentication service with the stored data, and

in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred (Paragraph [0069] teaches writing attack events to a system log and comparing new events to the log to determine if the new events constitute normal or abnormal behavior).

Claims 14, 20, 40 discloses the method of claim 1, wherein said searching the stored data to identify at least one of the plurality of the requests comprises searching the

stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts (Paragraph [0110] teaches different sensitivity levels according to types of attacks), and a time interval during which one or more requests are communicated (Paragraph [0061] where the number of events from a single source are compared to a threshold); wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables (Paragraph [0083] and [0084] teach the signature files organized according to type of attack).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 4, 6, 7, 18, 19, 28 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruton, III et al. (US 2003/0145225)** herein referred to as Bruton; as applied to claims **1-3, 5, 8-10, 13-17, 20-22, 25-27, 29, 30, 32-34, 36-38, and 40** above, and further in view of **Brock et al. (US 2003/0009693)** herein referred to as Brock. Bruton teaches the limitations of claim 3 as rejected above. Bruton does not teach but Brock teaches **claim 4** which discloses the method of claim 3, wherein said storing the

data relating to the plurality of the requests comprises storing a password associated with the one of the plurality of the requests if the one of the plurality of the requests is unsuccessful (Bruton paragraph [0004] wherein the pattern of bits is interpreted to be the password associated with the password log-on failure). It would be obvious to one of ordinary skill in the art at the time of invention to count the number of times a user tries unsuccessfully to log-on. The motivation to combine would be in Bruton paragraph [0004], which teaches that the number of log-on attempts is counted and compared against a threshold of events. If the attempts are above the threshold, it is determined to be an intrusion attempt and defensive actions are taken as stated.

Bruton teaches the limitations of claim 1 as rejected above. Bruton does not teach but Brock teaches **claims 6 and 19**, which discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple passwords to unsuccessfully attempt at least a predetermined quantity of requests on a single user account within a predefined time interval; using the multiple passwords to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the single user account within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests on the single user account within the predefined time interval (Bruton paragraph [0004] wherein the pattern of bits is interpreted to be the password associated with the password log-on failure. Paragraph [004] also compares the number of times the log-on is unsuccessfully attempted within a certain time period.)

It would be obvious to one of ordinary skill in the art at the time of invention to count the number of times a user tries unsuccessfully to log-on. The motivation to combine would be in Bruton paragraph [0004], which teaches that the number of log-on attempts is counted and compared against a threshold of events. If the attempts are above the threshold, it is determined to be an intrusion attempt and defensive actions are taken as stated.

Bruton teaches the limitations of claim 1 as rejected above. Bruton does not teach but Brock teaches **claims 7, 18, 28 and 35**, which disclose the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: a single password to unsuccessfully attempt at least a predetermined quantity of requests from multiple network addresses on a single user account within a predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the multiple network addresses on the single user account (Brock paragraphs [0031] and [0032] which teaches multiple intrusion attacks at different levels of importance). It would be obvious to one of ordinary skill in the art at the time of invention to compare the multiple intrusion attempts against the level of importance stored in the security policy. The motivation is Brock paragraph [0006], which teaches the importance of taking into account the historical data of attacks.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 11, 12, 23, 24, 31, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruton, III et al. (US 2003/0145225)** herein referred to as Bruton as applied to claims 1-3, 5, 8-10, 13-17, 20-22, 25-27, 29, 30, 32-34, 36-38, 40 above, and further in view of **Tumey et al. (US 2002/0097145)** herein referred to as Tumey.

Bruton teaches the limitations of claim 1 as rejected above. Bruton does not teach but Tumey teaches **claims 11 and 23**, which disclose the method of claim 1, wherein the plurality of the requests comprises one or more of the following types of requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated (Tumey paragraph [0033] where the human facial image data is interpreted to be the human interaction proof used for authentication). It would be obvious to one of ordinary skill in the art at the time of invention to use the biometric security of Tumey in the intrusion detection system of Bruton. The motivation to combine is in Tumey paragraph [0005]

which teaches that facial recognition is noninvasive security to the user and effective at all times.

Bruton teaches the limitations of claim 1 as rejected above. Bruton does not teach but Tumey teaches **claims 12, 24, 31, and 39** which disclose the method of claim 11, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to unsuccessfully attempt at least the predetermined quantity of the requests on multiple human interaction proof strings within the predefined time interval (Tumey paragraphs [0070] and [0071] which teach the use of multiple images to create a threshold for authentication. If the image does not fall within the threshold, it is discarded). It would be obvious to one of ordinary skill in the art to use multiple images to create a threshold for authentication. The motivation would be in Tumey paragraph [0072] which teaches that images may have erroneous verification results to do poor presentation of the user to the system's camera. It is best to create a threshold so as to create the best image for the security of the user.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
8/3/2007

S. Young
SYED A. ZIA 18/15/2007
PRIMARY EXAMINER